

Breach, AG

From: Belton, James A. <jbelton@bakerlaw.com>
Sent: Tuesday, August 26, 2014 6:28 PM
To: Breach, AG
Cc: Forsheit, Tanya; Koller, M. Scott
Subject: Incident Notification
Attachments: Imhoff Agency Notification - CT.PDF

Please see attached sent on behalf of Tanya Forsheit.

Web site

T 310.442.8820 James Belton
F 310.820.8859 Legal Secretary
www.bakerlaw.com jbelton@bakerlaw.com

BakerHostetler
11601 Wilshire Boulevard
Suite 1400
Los Angeles, CA 90025-0509

BakerHostetler

This email is intended only for the use of the party to which it is addressed and may contain information that is privileged, confidential, or protected by law. If you are not the intended recipient you are hereby notified that any dissemination, copying or distribution of this email or its contents is strictly prohibited. If you have received this message in error, please notify us immediately by replying to the message and deleting it from your computer.

Internet communications are not assured to be secure or clear of inaccuracies as information could be intercepted, corrupted, lost, destroyed, arrive late or incomplete, or contain viruses. Therefore, we do not accept responsibility for any errors or omissions that are present in this email, or any attachment, that have arisen as a result of e-mail transmission.



Baker&Hostetler LLP

11601 Wilshire Boulevard
Suite 1400
Los Angeles, CA 90025-0509
T 310.820.8800
F 310.820.8859
www.bakerlaw.com

Tanya Forsheit
direct dial: 310-442-8831
tforsheit@bakerlaw.com

August 26, 2014

VIA E-MAIL at ag.breach@ct.gov

Office of the Connecticut Attorney General
Consumer Protection Division
55 Elm Street
Hartford, CT 06106

Re: Incident Notification

Dear Sir or Madam:

Our client, Imhoff and Associates, P.C. ("Imhoff"), learned on June 27, 2014, that a hard drive containing backup files for one of the firm's servers was stolen from the locked trunk of an employee's vehicle. Imhoff immediately notified the Santa Monica Police Department and began a thorough internal investigation to determine what information was contained on the hard drive.

After a detailed review with outside computer forensic experts, Imhoff confirmed that the hard drive may have contained files with differing amounts of employee and client information, including name, Social Security number, driver's license number and contact information (e.g., email address, mailing address and phone number). Imhoff has been working with law enforcement, but to date, has been unable to locate the hard drive.

Imhoff has no reason to believe that the hard drive was stolen for the information it contained or that the information has been misused in any way. Although the hard drive was not encrypted, special software would be required in order to read most of the information on the hard drive. Still, as a precaution, Imhoff will begin notifying individuals affected by the incident on August 26, 2014 and is offering them one year of complimentary credit monitoring and identity theft protection services through AllClear ID. Imhoff is also providing call center support for those affected.

To help prevent something like this from happening in the future, Imhoff is strengthening its encryption processes and enhancing its policies, procedures and staff education regarding the safeguarding of firm property and information.

Chicago Cincinnati Cleveland Columbus Costa Mesa
Denver Houston Los Angeles New York Orlando Washington, DC

Office of the Connecticut Attorney General
August 26, 2014
Page 2

Attached hereto is a sample copy of the notification letter being sent to affected residents. Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,


Tanya Forsheit

Enclosure



Processing Center · P.O. Box 3825 · Suwanee, GA 30024

August 26, 2014



John Q Sample
123 Main Street
Anytown, US 12345-6789

Dear John Q Sample:

Imhoff and Associates, PC ("Imhoff") is writing to inform you of an incident involving a theft of a backup hard drive that may have contained some of your information.

What happened?

During the early morning hours on June 27, 2014, a hard drive containing backup files for one of the firm's servers was stolen from the locked trunk of an employee's vehicle. The employee discovered the theft later that day and immediately notified the Santa Monica Police Department. We have been working with law enforcement but, to date, they have been unable to locate the stolen hard drive.

Imhoff also immediately began an internal investigation to determine what information was contained on the hard drive. Working with outside computer forensic experts, we have confirmed that the hard drive may have contained your name, birthday, Social Security number, driver's license number, and contact information, such as your home address, e-mail and phone number.

What is Imhoff and Associates doing to protect me?

Imhoff has no reason to believe that the hard drive was stolen for the information it contained or that your information has been accessed or used in any way. However, as a precaution, we have arranged to have AllClear ID help you protect your identity for 12 months at no cost to you. The following identity protection services will be available to you beginning on the date of this notice, and you can use them at any time during the next 12 months.

AllClear SECURE: The team at AllClear ID is ready to work with you to protect your identity. Because you are receiving this letter, you are eligible to use the AllClear SECURE service if you so choose. If a problem arises, simply call (877) 615-3769 and a dedicated investigator will assist you in attempting to recover financial losses and take steps to help restore your credit and identity to their proper condition. AllClear maintains an A+ rating at the Better Business Bureau.

AllClear PRO: This service offers you additional layers of protection including credit monitoring and a \$1 million identity theft insurance policy. If you would like to use the AllClear PRO service, you will need to provide your personal information to AllClear ID. You may sign up for the AllClear PRO service online at enroll.allclearid.com or by phone by calling (877) 615-3769 using the following redemption code: 9999999999.

Please note: Additional steps may be required by you in order to activate your phone alerts.

We also recommend that you carefully check your credit reports for accounts you did not open or for inquiries from creditors you did not initiate. If you see anything you do not understand, call the credit agency immediately. If you find any suspicious activity on your credit reports, call the police. Also, please review the enclosed "Information



about Identity Theft Protection" reference guide on the back of this letter, which describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

What is Imhoff and Associates doing to prevent this from happening in the future?

To help prevent something like this from happening in the future, we are strengthening our internal processes with respect to encryption and enhancing our policies, procedures and staff education regarding the safeguarding of company property and information.

If you have further questions or concerns about this incident, please call (877) 615-3769, Monday through Saturday, 8:00 a.m. to 8:00 p.m. Central Standard Time (closed on U.S. observed holidays). We sincerely regret any inconvenience or concern caused by this incident.

Sincerely,



Vincent M. Imhoff
Managing Director
Imhoff & Associates, PC

Information about Identity Theft Protection

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax
P.O. Box 740241
Atlanta, GA 30374-0241
800-685-1111
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
888-397-3742
www.experian.com

TransUnion
P.O. Box 6790
Fullerton, CA 92834-6790
800-916-8800
www.transunion.com

You should remain vigilant with respect to reviewing your account statements and credit reports, and you should promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding and protection against identity theft: Federal Trade Commission, Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft.

Fraud Alerts: There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies at the toll-free numbers listed below:

Equifax
877-478-7625

Experian
888-397-3742

TransUnion
800-680-7289

Credit Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally \$5 to \$20 per action at each credit reporting company. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information.

Equifax
P.O. Box 105788
Atlanta, GA 30348
www.equifax.com

Experian
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion
Fraud Victim Assistance Division
P.O. Box 6790
Fullerton, CA 92834-6790
www.transunion.com

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.

